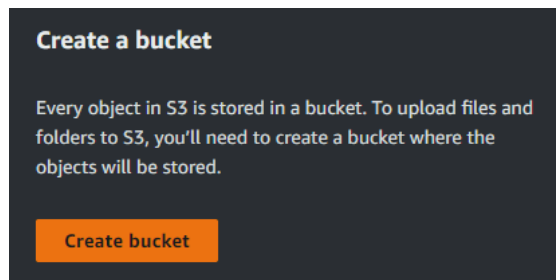


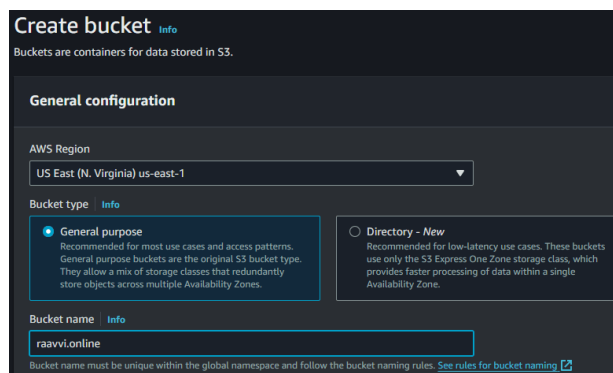
# AWS DOCUMENTATION(ROUTE 53)

## Creating the Public Bucket and hosting the static website using route 53.

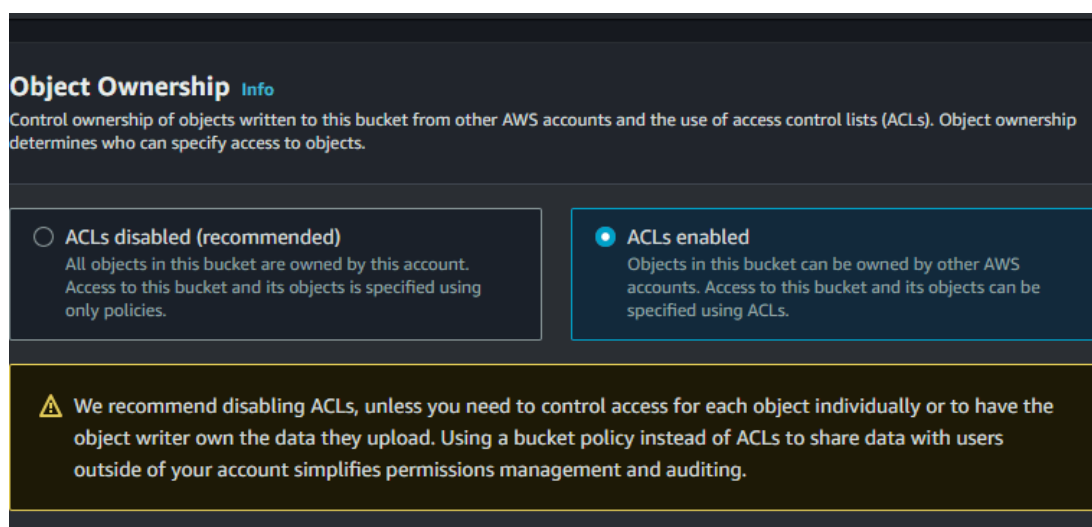
Step I : go to S3 service and click on create bucket.



Step II : then select region and give the name to the bucket.



Step III : enable the ACL.



Step IV : then untick block all public access.

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)


☐ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

 **Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.


Step V : then click on create Bucket.

**Bucket Key**  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

► **Advanced settings**

 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

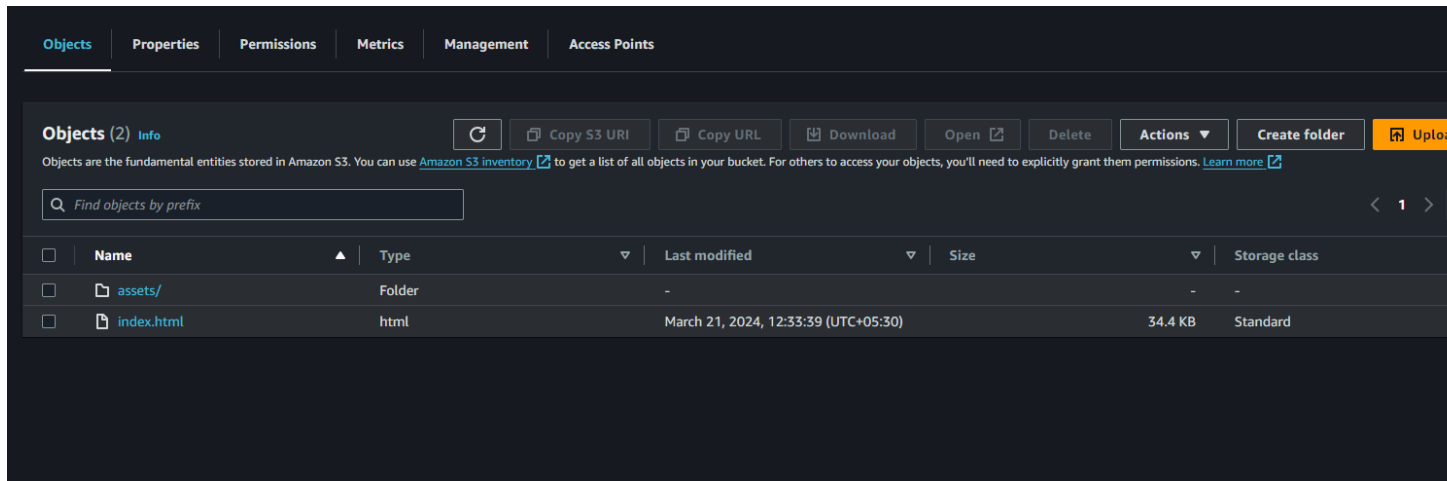
Cancel **Create bucket**

Step VI : go to browser, and search css free template select it and download it.

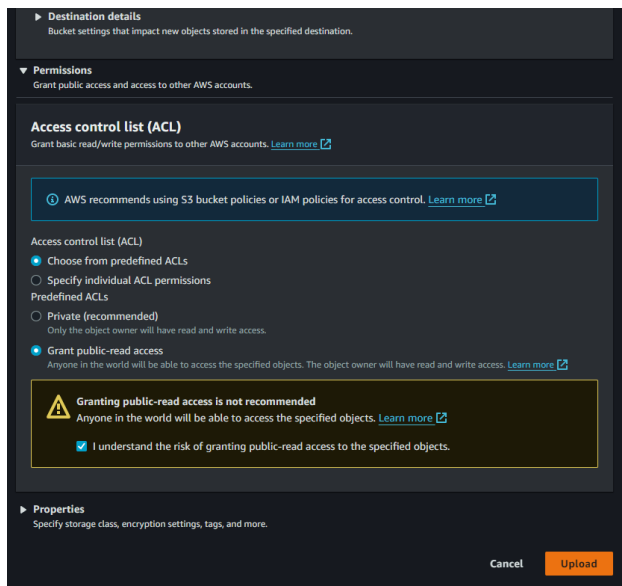
Step VII : then unzip it.

Step VIII : and upload the files and folders in Bucket.

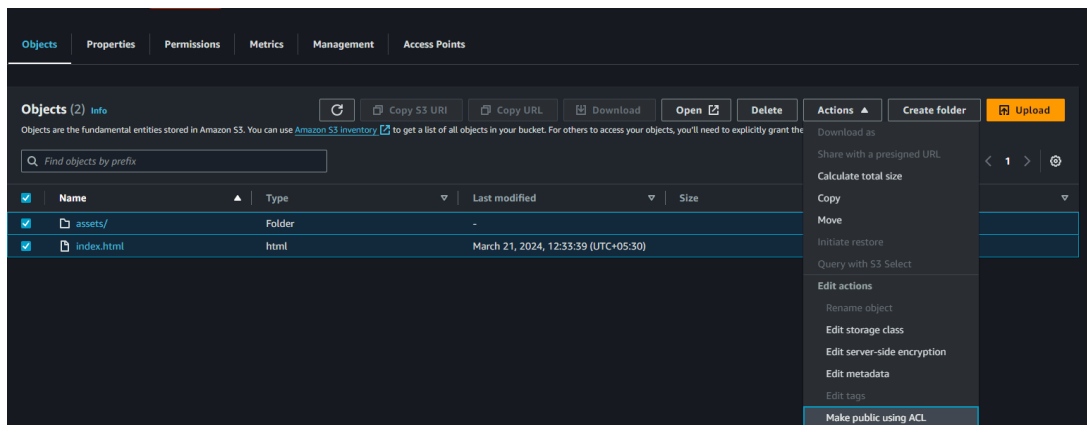
Step IX : after that click on upload.



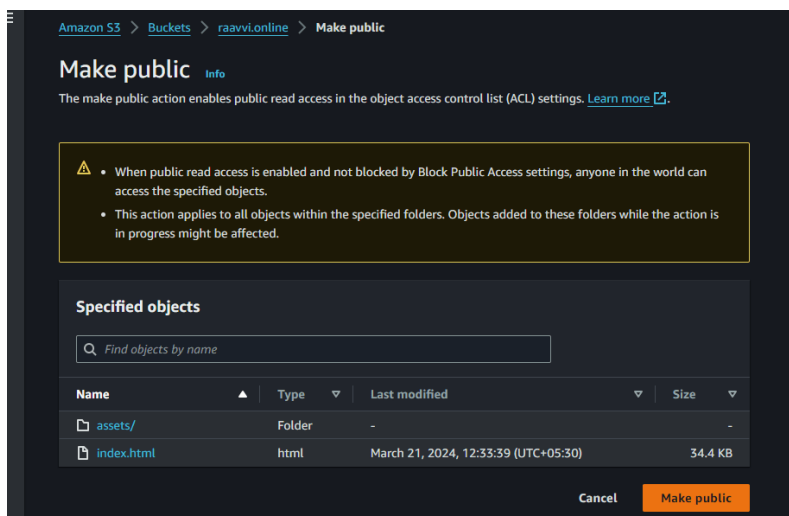
Step X : In Permissions, Grant the public-read access and upload it.



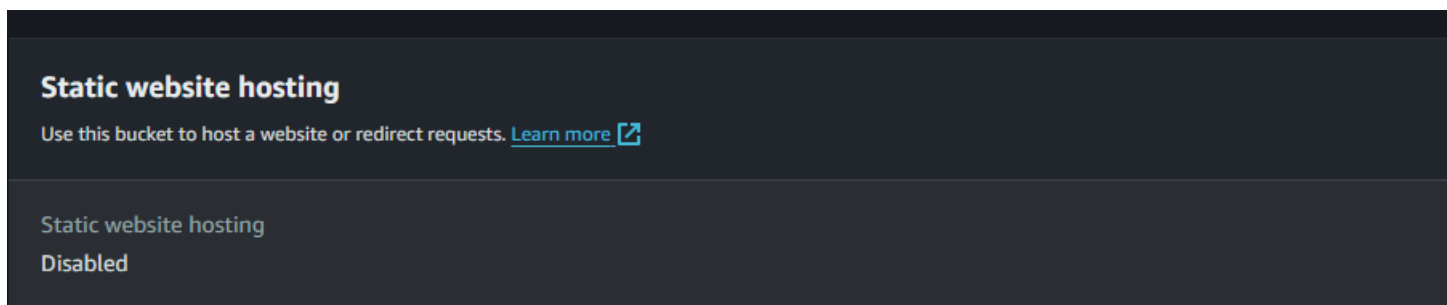
Step XI : then Select all objects and click on Action and click on the Make public using ACL.



Step XII : then click on Make public.



Step XIII : In Properties, click on edit in Static web Hosting and enable it.



Step XIV : In ACL click on edit and give permission List and Read to Everyone(public Access) and click on save changes.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)



The console displays combined access grants for duplicate grantees  
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: fe3528bd8f1087f605d1d182a652a77ac64e774830321b672bae2a474df5447f	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group	<input type="checkbox"/> List	<input type="checkbox"/> Read

Group:  
http://acs.amazonaws.com/groups/s3/LogDelivery

- ⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.

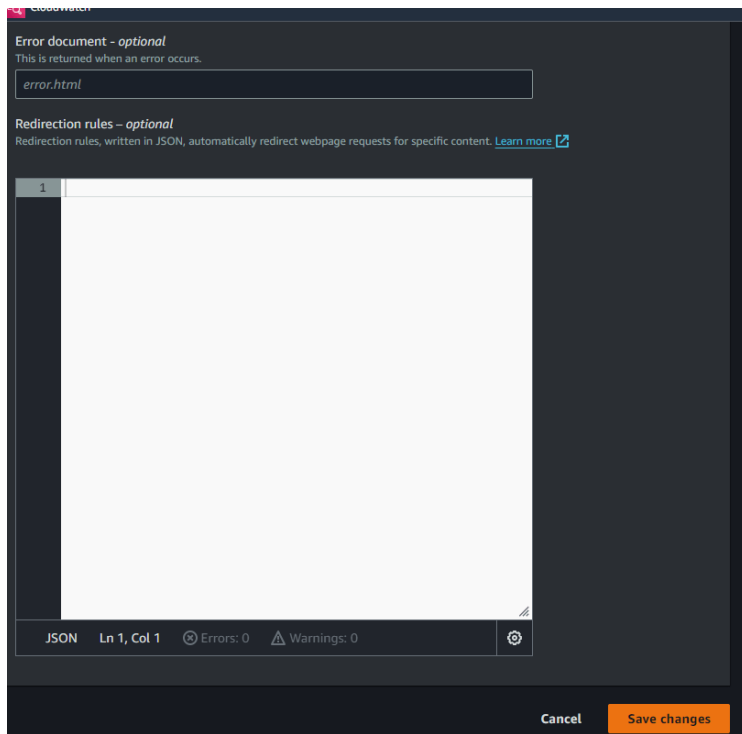
[Learn more](#)

☒ I understand the effects of these changes on my objects and buckets.

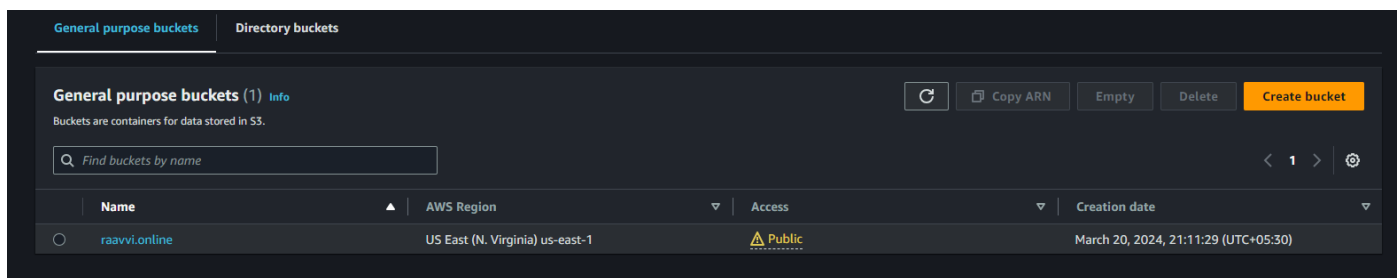
Access for other AWS accounts  
No other AWS accounts associated with the resource.

Add grantee

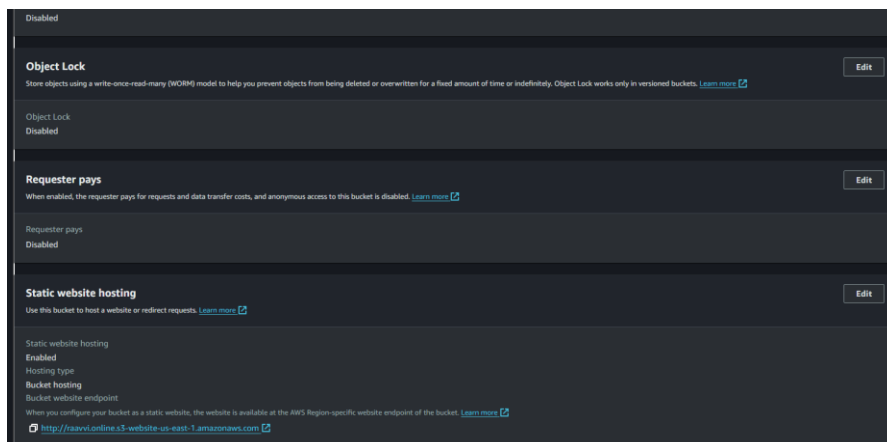
Cancel Save changes



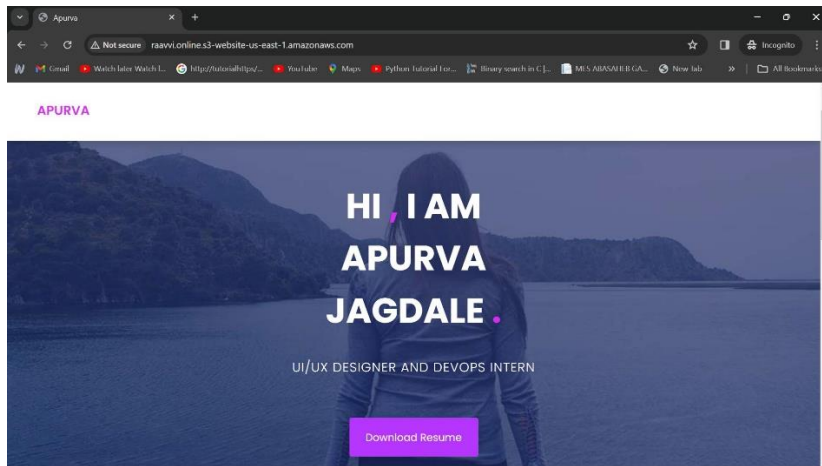
Step XV : See here, bucket is public.



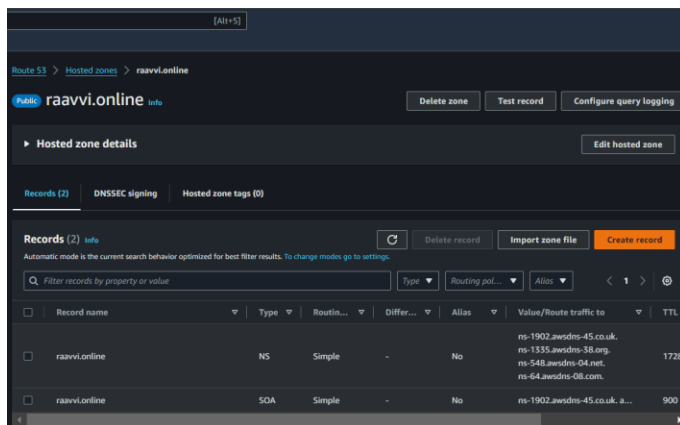
Step XVI : then copy the link in Static web hosting and paste it in other browser.



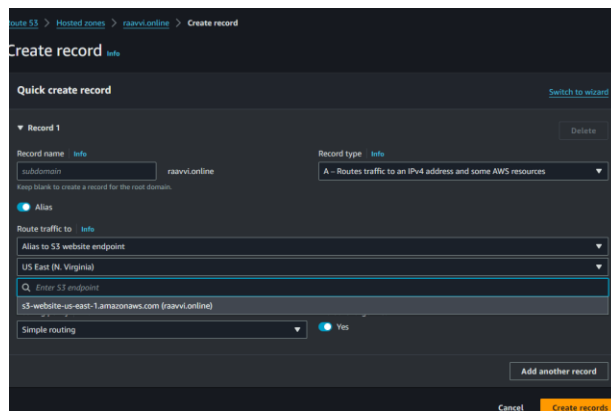
Step XVII : See here, the website is hosted properly.



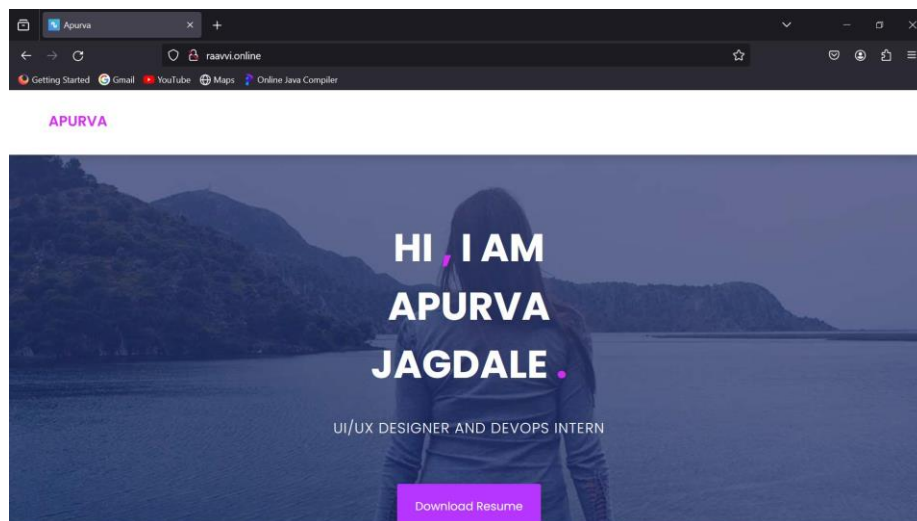
Step XVIII : then go Route 53 service and go to created hosted zone and delete previous uploaded record and click on create record.



Step XIX : then select the record type A, enable Alias. In Route traffic to select the Alias to S3 website endpoint, select region and endpoint and click on create records.



Step XX: and search the domain name in browser, here we see static website hosted properly using route 53.



## PUBLIC HEALTH IN ROUTE 53

Step I : Create the Instance in Sydney Region give the http and add the script in it and Launch instance

```
#!/bin/bash
```

```
sudo -i
```

```
yum install httpd -y
```

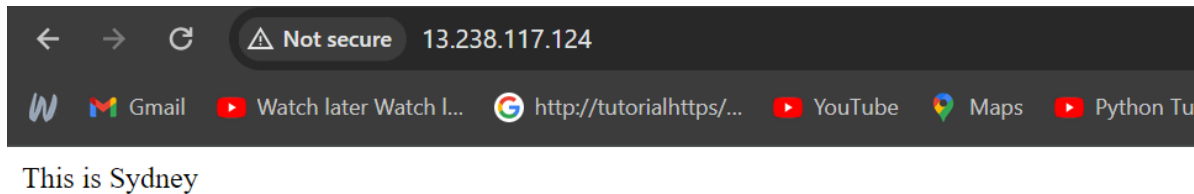
```
systemctl start httpd
```

```
systemctl enable httpd
```



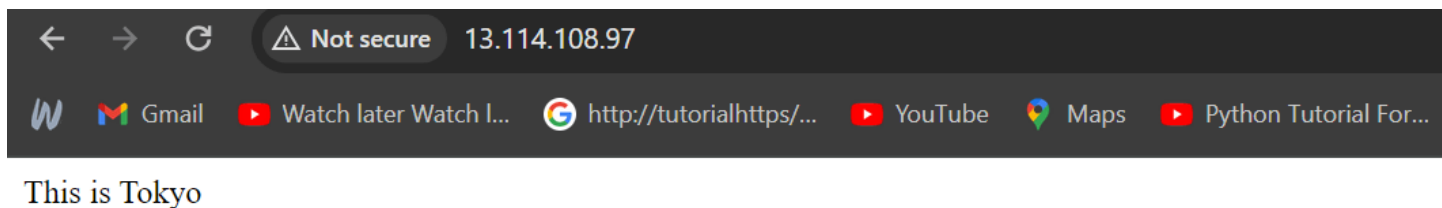
echo "This is Sydney" > /var/www/html/index.html

Step II : copy the public IP and paste it in other browser.

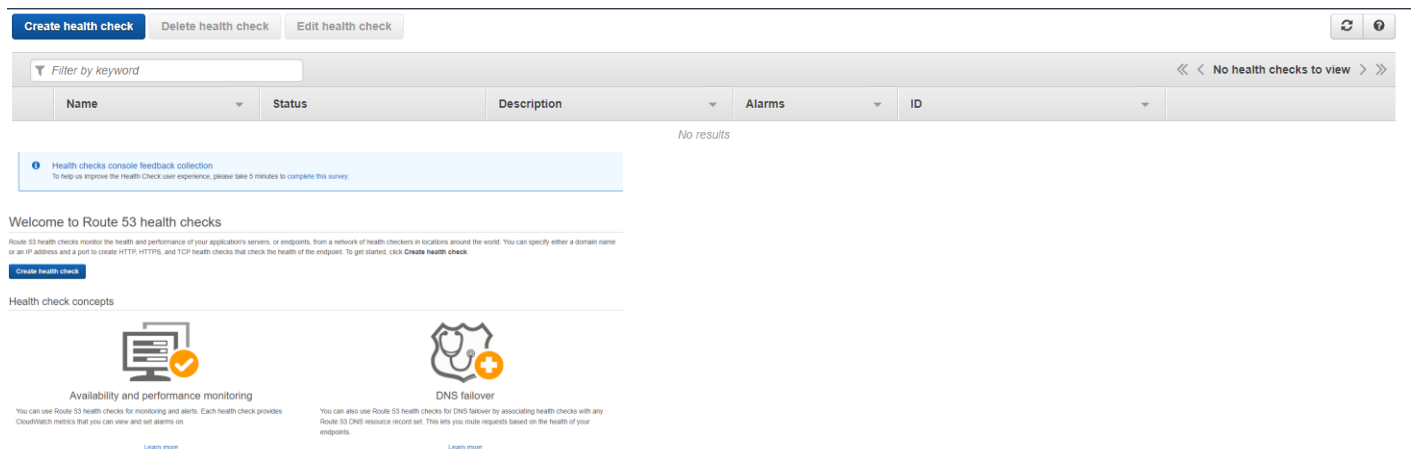


Step III: Follow same step to Launch instance in Tokyo.

Step IV : then copy the public ip and paste it in other browser.



Step V : go to Route 53 and click on Create Health Check.



Step VI : give the name and select endpoint in what to monitor.

Step VII : then Select the specify endpoint by IP address ,give IP address, give host Name.

**Configure health check**

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name

What to monitor ☒ Endpoint ☐ Status of other health checks (calculated health check) ☐ State of CloudWatch alarm

Monitor an endpoint

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy. [Learn more](#)

Specify endpoint by ☒ IP address ☐ Domain name

Protocol

IP address \*

Host name

Port \*

Path

Advanced configuration

URL <http://13.114.108.97:80/>

Step VIII : and click on next.

Path

Advanced configuration

Request interval ☒ Standard (30 seconds) ☐ Fast (10 seconds)

Failure threshold \*

String matching ☒ No ☐ Yes

Latency graphs

Invert health check status

Disable health check ☐ By default, disabled health checks are considered healthy. [Learn more](#)

Health checker regions ☐ Customize ☒ Use recommended

- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- South America (São Paulo)

URL <http://13.114.108.97:80/>

Health check type [Basic](#) - no additional options selected ([View Pricing](#))

\* Required Cancel Next

Step IX : then, click on create health check.

Get notified when health check fails

If you want CloudWatch to send you on-demand (free) notifications, such as an email, when the status of the health check changes to unhealthy, create an alarm and specify where to send notifications.

Create alarm ☐ Yes ☒ No

\* Required Cancel Previous Create health check

Step X : follow same process and create other health check using other instance IP .

**Configure health check**

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name

What to monitor ☒ Endpoint ☐ Status of other health checks (calculated health check) ☐ State of CloudWatch alarm

Monitor an endpoint

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy. [Learn more](#)

Specify endpoint by ☒ IP address ☐ Domain name

Protocol

IP address \*

Host name

Port \*

Path

Advanced configuration

URL <http://13.236.117.124:80/>

Advanced configuration

Request interval: ☒ Standard (30 seconds) ☐ Fast (10 seconds)

Failure threshold:

String matching: ☒ No ☐ Yes

Latency graphs: ☐

Invert health check status: ☐

Disable health check: ☐ By default, disabled health checks are considered healthy. [Learn more](#)

Health checker regions: ☐ Customized ☒ Use recommended

- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- South America (São Paulo)

URL:

Health check type: Basic - no additional options selected (View Pricing)

\* Required Cancel Next

## Get notified when health check fails ?

If you want CloudWatch to send you an Amazon SNS notification, such as an email, when the status of the health check changes to unhealthy, create an alarm and specify where to send notifications.

Create alarm ☐ Yes ☒ No

\* Required Cancel Previous Create health check

Step XI : see here, after refreshing the instances status are healthy here.

✔ Health check with id 99347b45-53b0-4c47-839a-862786eb3fa0 has been created successfully

Create health check
Delete health check
Edit health check

Filter by keyword

Name	Status	Description	Alarms	ID
<input type="checkbox"/> tokyo	<span style="color: green;">Healthy</span>	http://13.114.108.97:80/	No alarms configured.	5d030ebb-c3ce-4667-a710-a06b149eaba4
<input type="checkbox"/> sydney	<span style="color: green;">Healthy</span>	http://13.238.117.124:80/	No alarms configured.	99347b45-53b0-4c47-839a-862786eb3fa0

To monitor two health check Instance

Step XII : Create the Health check give name it status, select Status of other health check in What to monitor.

Configure health check ?

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name:

What to monitor: ☐ Endpoint ☒ Status of other health checks (calculated health check) ☐ State of CloudWatch alarm

Monitor other health checks (calculated health check)

The health of this health check depends on the status of the following health checks:

Health checks to monitor:

Report healthy when: ☐ at least 1 of 2 selected health checks are healthy ☐ all health checks are healthy (AND) ☒ one or more health checks are healthy (OR)

Invert health check status: ☐

Disable health check: ☐ By default, disabled health checks are considered healthy. [Learn more](#)

Health check type: Basic - no additional options selected (View Pricing)

Step XIII : then select the one or more health check are health (OR) in Report healthy when. And then click on next.

Configure health check

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name

status

What to monitor

☐ Endpoint

☒ Status of other health checks (calculated health check)

☐ State of CloudWatch alarm

Monitor other health checks (calculated health check)

The health of this health check depends on the status of the following health checks:

Health checks to monitor

tokyo

sydney

Report healthy when

☐ at least 1 of 2 selected health checks are healthy

☐ all health checks are healthy (AND)

☒ one or more health checks are healthy (OR)

Invert health check status

☐

Disable health check

☐ By default, disabled health checks are considered healthy. [Learn more](#)

Health check type

Basic - no additional options selected [\(View Pricing\)](#)

Required

Cancel

Next

Step XIV : then click on create health check.

Get notified when health check fails

If you want CloudWatch to send you an Amazon SNS notification, such as an email, when the status of the health check changes to unhealthy, create an alarm and specify where to send notifications.

Create alarm

☐ Yes

☒ No

\* Required

Cancel

Previous

Create health check

Step XV : See here the Instances are healthy states that's why here status is healthy.

Health check with id 56af0568-b02d-4ca4-ba5d-d38f909907c has been created successfully

Name	Status	Description	Alarms	ID
<input type="checkbox"/> status	Healthy	Calculated threshold: 1 of 2	No alarms configured.	56af0568-b02d-4ca4-ba5d-d38f909907c
<input type="checkbox"/> tokyo	Healthy	http://13.114.108.97:80/	No alarms configured.	5d030ebb-cbce-4667-a710-a06b149eab44
<input type="checkbox"/> sydney	Healthy	http://13.236.117.124:80/	No alarms configured.	99347b45-53b0-4c47-839a-862786eb39d0

Step XVI : then edit the status health check and select the report healthy in all checks are healthy(AND) then go to instance in Sydney region connect it and stop the httpd service. Here the instance is not work.

Health checks > 56af0568-b02d-4ca4-ba5d-d38f909907c

Configure health check

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name

What to monitor Status of other health checks (calculated health check)

The health of this health check depends on the status of the following health checks:

Health checks to monitor

Report healthy when ☐ at least 2 of 2 selected health checks are healthy ☒ all health checks are healthy (AND) ☐ one or more health checks are healthy (OR)

Invert health check status ☐

Disable health check ☐ By default, disabled health checks are considered healthy. [Learn more](#)

\* Required Cancel Save

Step XVII : then go to instance in Sydney region connect it and stop the httpd service. Here the instance is not work.

```

#_
~\_#####_
~~\_#####\
~~\_###|
~~\_#|
~~V~'-'>
~~~~
~~~.~.
~/m/'
[ec2-user@ip-172-31-6-166 ~]$ sudo systemctl stop httpd

```

Amazon Linux 2023

<https://aws.amazon.com/linux/amazon-linux-2023>

Step XVIII : here it follows the given condition if one health check is unhealthy then its shows the unhealthy status.

Create health check Delete health check Edit health check

Filter by keyword

	Name	Status	Description	Alarms	ID
<input type="checkbox"/>	status	15 minutes ago now Unhealthy	Calculated threshold: 2 of 2	No alarms configured.	56af0568-b02d-4ca4-ba5d-d38f909907c
<input type="checkbox"/>	tokyo	15 minutes ago now Healthy	http://13.114.108.97:80/	No alarms configured.	5d030ebb-cbce-4667-a710-a06b149eaba4
<input type="checkbox"/>	sydney	12 minutes ago now Unhealthy	http://13.238.117.124:80/	No alarms configured.	99347b45-53b0-4c47-839a-862786eb3fa0

<< < 1 to 3 of 3 health checks